Two major areas of interest have comments included below:
HIPAA's application to schools and educational programs
HIPAA and the Graham-Leach Bliley Bill

With relation to the application of HIPAA to our schools and educational programs, the first e-news item has some important interpretations, including: "...However, to the extent a school clinic is within the definition of a health care provider, as Congress defined the term, and the school clinic is engaged in HIPAA transactions, it will be a covered entity and must comply with the rules below." Be sure to read the note for context.

Enjoy!!!
Ken

TOPIC LIST:

********* [hipaalive] RE: GENERAL: FERPA and student health services **********

>>> tom.hanks@beaconpartners.com 03/28/01 10:10AM >>>
*** This is HIPAAlive! From Phoenix Health Systems ***

The Privacy rule appears clear that the exemption pertains only to Federally Funded Education Institution and only to information in student education records that are restricted to viewing by providers.

Note 1: You need to be careful about understanding when student health records may be considered student education records.
Note 2: The provider component of an educational institution that provides treatment to the student would still be a covered entity and any protected health information created or maintained by the provider component would covered - as long as the provider component conducted electronic transactions.

See Page 82483 for the DHHS discussion of FERPA - I have included some excerpts.

"We have excluded education records covered by FERPA, including those education records designated as education records under Parts B, C, and D of the Individuals with Disabilities Education Act Amendments of 1997, from the definition of protected health information. For example, individually identifiable health information of
students under the age of 18 created by a nurse in a primary or secondary school that receives federal funds and that is subject to FERPA is an education record, but not protected health information. Therefore, the privacy regulation does not apply. of privacy protection for his/her individually identifiable health information, Congress did not provide us with authority to disturb the scheme it had devised for records maintained by educational institutions and agencies under FERPA. We do not believe Congress intended to amend or preempt FERPA when it enacted HIPAA. "

- And-

"We have also excluded certain records, those described at 20 U.S.C. 1232g(a)(4)(B)(iv), from the definition of protected health information because FERPA also provided a specific structure for the maintenance of these records. These are records (1) of students who are 18 years or older or are attending post-secondary educational institutions, (2) maintained by a physician, psychiatrist, psychologist, or recognized professional or paraprofessional acting or assisting in that capacity, (3) that are made, maintained, or used only in connection with the provision of treatment to the student, and (4) that are not available to anyone, except a physician or appropriate professional reviewing the record as designated by the student. Because FERPA excludes these records from its protections only to the extent they are not available to anyone other than persons providing treatment to students, any use or disclosure of the record for other purposes, including to exercise his/her access rights. The provider, then, would need to treat the record in accordance with FERPA's requirements and be relieved from its obligations under the privacy regulation. We chose not to adopt this approach because it would be unduly burdensome to require providers to comply with two different, yet similar, sets of regulations and inconsistent with the policy in FERPA that these records be exempt from regulation to the extent the records were used only to treat the student."

-And-

"The Family Educational Rights and Privacy Act FERPA, as amended, 20 U.S.C. 1232g, provides parents of students and eligible students (students who are 18 or older) with privacy protections and rights for the records of students maintained by These exclusions are not applicable to all schools, however. If a school does not receive federal funds, it is not an educational agency or institution as defined by FERPA. Therefore, its records that contain individually identifiable health information are not

education records. These records may be protected health information. The educational institution or agency that employs a school nurse is subject to our regulation as a health care provider if the school nurse or the school engages in a HIPAA transaction."

- Also see page 82595 -

"...However, to the extent a school clinic is within the definition of a health care provider, as Congress defined the term, and the school clinic is engaged in HIPAA
transactions, it will be a covered entity and must comply with the rules below."

I hope this helps,

Thanks,

Tom Hanks
Practice Director, Enterprise Security & HIPAA Compliance
Beacon Partners, Inc.

********** [hipaalive] HIPAA and the Graham-Leach Bliley Bill **********

>>> IMGLEADER@aol.com 03/29/01 08:18AM >>>
*** This is HIPAAlive! From Phoenix Health Systems ***

Charlene:
If you read, the preamble to the final G-L-B Privacy Rule (published 5/24/00), which is available online, at http://www.ftc.gov you will understand the FTC's perspective as to HIPAA overlap, and according to them their agenda includes the bank/healthcare interface.
Dick Kadas

>>> CLohmeie@xantushealthplan.com 03/29/01 07:15AM >>>
*** This is HIPAAlive! From Phoenix Health Systems ***

In Tennessee, I contacted a lawyer in our state Department of Commerce and Insurance. He knew exactly what I was talking about.

His department is in charge of writing the state regulation to comply with Gramm-Leach. He said the regs here should be written soon...regardless of when the regs become final the compliance date will not change. I am assuming the supercede rule will apply if the regs written by the state are more strict or less strict than HIPAA. I won't be able to check that out

until the state regs are final.

Hope that points you in the right direction.

>>> MWorek@GatewayHealthPlan.com 03/29/01 07:54AM >>>
*** This is HIPAAlive! From Phoenix Health Systems ***

Compliance depends on the regulations set in your state. The compliance date of 7/1/01 has not been changed, but it is up to each state to issue regulations implementing the requirements of the bill. However, G-L-B does not apply to healthcare institutions, just healthcare payers and financial institutions.

In Pennsylvania, the payers lobbied the department of insurance and PA's DOI exempted health payers from the regulations because of HIPAA and because they didn't feel that this was original intent of the law.

********** [hipaalive] HIPAA in Correctional Facilities **********
*** This is HIPAAlive! From Phoenix Health Systems ***

I am the HIPAA Project Manager for the County of Orange Health Care Agency in California. I noticed a brief discussion regarding correctional facilties a while back and am interested in any more thoughts. Tom had suggested that many medical components of a correctional facilty wouldn't conduct electronic transactions, but I think this really depends on how they are organized. Our Agency provides all of the health care to adult and juvenile inmates as County operated program (good case for a hybrid entity). There are a number of circumstances where electronic transactions are implemented to include Medi-Cal and MediCare billing, transactions with contracted hospitals for in-patient care,etc. Further, it doesn't appear that the privacy rules are significantly different than those already in existence for the State regarding disclosure of PHI to correctional facility personnel when required for the safety of the institution and so on...I would love to hear from any other County or similar organizations and thoughts regarding the multiple complexities of a government run entity.
Kevin Van Otterloo
HIPAA Project Manager
Orange County Health Care Agency, CA
(714) 667-8366
kvanotterloo@hca.co.orange.ca.us

********** [hipaalive] Sharing Info - Electronic radiology related images **********
>>> tom.hanks@beaconpartners.com 03/29/01 11:02PM >>>

*** This is HIPAAlive! From Phoenix Health Systems ***

I think your impression is correct. For the purpose of treatment providers should have access to patient records that are not their patients. For example, it would not be unreasonable for a provider to need access to other patients' records with similar symptoms/diagnosis to compare images, MRI, CT, and other test results for the purpose of comparative diagnosis. This could also be true for comparison of treatment protocols and outcomes.

Thanks,

Tom Hanks
Practice Director, Enterprise Security & HIPAA Compliance
Beacon Partners, Inc.

********** HHS Announces Plans to Revise Medical Privacy Rule; **********
********** NGA Urges States to Comment Before March 30 Deadline **********
>>> "Cohen, Burt (CHHS)" <BCohen@chhs.ca.gov> 03/28/01 10:35AM >>>
-----Original Message-----
From: Testa, Kristen (CHHS)
Sent: Wednesday, March 28, 2001 9:52 AM
To: Cohen, Burt (CHHS); Maxwell-Jolly, David (CHHS)
Cc: Rosenstein, Stan (DHS-MCS); 'jgrgurina@mrmib.ca.gov'; 'sshewry@mrmib.ca.gov'
Subject: FW: HHS Announces Plans to Revise Medical Privacy Rule; NGA Urges Sta tes to Comment Before March 30 Deadline
Importance: High

-----Original Message-----
From: Scism, Cherilyn [mailto:CScism@NGA.ORG]way
Sent: Wednesday, March 28, 2001 7:21 AM
To: .....
Subject: HHS Announces Plans to Revise Medical Privacy Rule; NGA Urges Sta tes to Comment Before March 30 Deadline
Importance: High

HHS Announces Plans to Revise Medical Privacy Rule; NGA Urges States to Comment Before March 30 Deadline

On March 27, Secretary of Health and Human Services (HHS) Tommy Thompson
announced his intention to "simplify" regulations concerning medical record privacy. He indicated an interest in "lessening the financial burden the rule will have on providers." Thompson indicated that the new rule would be

issued as a "final rule with amendments," in the Federal Register, but did not provide further information on the content or timing of such a rule.

States are strongly urged to submit comments on the Final Rule or, at least, to re-submit their comments on the proposed rule. Comments will be considered if received no later than 5 p.m. on March 30, 2001. Comments can be submitted to: U.S. Department of Health and Human Services, Attention: Privacy I, Room 801, Hubert H. Humphrey Building, 200 Independence Avenue, SW., Washington, DC 20201 or online <http://aspe.hhs.gov/admnsimp/>.

Resources:
*NGA Website on Privacy
<http://www.nga.org/nga/lobbyIssues/1,1169,D_1384,00.html>
*HHS Press release <http://aspe.hhs.gov/admnsimp/FINAL/PRESS3.HTM>
*February 28, 2001 Federal Register Notice
<http://aspe.hhs.gov/admnsimp/FINAL/FR28fe01.htm>
*Final Rule in December 28, 2000 Federal Register
<http://www.access.gpo.gov/su_docs/fedreg/a001228c.html>

Cherilyn Cepriano Scism
Legislative Associate for Health Policy
National Governors' Association
office: (202) 624-5391

********** [hipaalive] Re: TCS - additional data elements **********
>>> dafeinberg@home.com 03/28/01 07:47AM >>>
*** This is HIPAAlive! From Phoenix Health Systems ***

Good morning,

I believe the message below from Stanley Nachimson of HCFA pretty much answers your questions.
As always, hope this helps a bit.

Dave Feinberg
Co-Chair, HIPAA Implementation Work Group
Insurance Subcommittee (X12N)
Accredited Standards Committee X12
Voting Member, HL7 and X12
Rensis Corporation [A Consulting Company]
206-617-1717
DAFeinberg@computer.org

= =
----- Original Message -----
From: "Stanley Nachimson" <SNachimson@hcfa.gov>
Sent: Tuesday, November 28, 2000 5:45 AM

Subject: Minimum and Maximum data element field lengths -Reply

Our interpretation has been that you must be able to accept and process transactions with data elements that meet the implementation guide (ie that fall anywhere from the minimum ot the maximum). Your system must be able to accept Address Information up to 55 bytes, and process it accordingly. If this comes in on a claim, you must be able to store the 55 bytes somewhere for forwarding on to the next payer in a COB situation.

********** April 2nd through 8th is National Public Health Week **********
>>> "McDaniel, Mike (DHS-ITSD)" <MMcdanie@dhs.ca.gov> 03/28/01 10:18AM >>>

April 2nd through 8th is National Public Health Week. For more information on statewide Public Health activities, please visit our web site at www.dhs.ca.gov/phweek <http://www.dhs.ca.gov/phweek>

Mike J. McDaniel - DHS - ITSD
744 P Street - Room 300
Phone (916)657-1564
FAX (916)654-5916
E-mail mmcdanie@dhs.ca.gov <mailto:mmcdanie@dhs.ca.gov>

********** HHS Secretary on Change of Privacy Rules **********
Politics - Associated Press - updated 12:26 PM ET Mar 28

Tuesday March 27 5:16 PM ET
Thompson Seeks Privacy Rule Changes

By LAURA MECKLER, Associated Press Writer

WASHINGTON (AP) - Health and Human Services (news - web sites) Secretary Tommy Thompson said Tuesday that he expects to make changes to Clinton administration medical privacy rules, responding to industry complaints about the potential cost.

In a wide-ranging session with reporters, Thompson also indicated that he would push for the Democratic approach to aiding the uninsured and said he's learning that as a cabinet secretary, he can't always speak his mind.

``I found out you have to check with everybody before you move,'' he said. ``I've already been in the dog house several times because I haven't done that.''

The medical privacy rules, several years in the making, establish the first federal right to privacy of medical records, requiring health care providers to get written permission before disclosing personal health information.

Health industry officials pressed for more flexibility before the rules were issued and saw another opportunity when Thompson took over HHS. They heavily lobbied him to revisit the issue, and last month, Thompson put the rules on hold, opening them up for another round of public comments.

On Tuesday, he promised that he would have a decision about changes by the end of April and report to Congress soon after.

``I am fairly certain at this point - without saying for sure - there will be some modifications to simplify and to lessen the financial burden,'' he told reporters. He added that he has heard from many people about ``the tremendous burden'' and ``the tremendous cost'' that the rules would impose.

Some privacy advocates have said they fear the delay will be indefinite. ``Let me reassure you, there will be a privacy rule,'' Thompson said.

On the uninsured, Thompson said he supports tax credits to help people buy private insurance policies, as President Bush (news - web sites) has proposed.

But he said he would also like to see an expansion of the Children's Health Insurance Program, which provides subsidized coverage to families directly, much like the program he created as Wisconsin governor. This is the approach that Democrats typically favor, and Bush did not include anything like it in his budget.

``We have to work under the guidelines that the president had included,'' Thompson said. ``But I'm going to be very supportive of initiatives in Congress'' that expand CHIP.

In the meantime, he said he will encourage officials in his department to approve more state experiments that allow for programs like Wisconsin's.

Thompson also said:

-On prescription drugs for Medicare: Congress is not likely to support Bush's plan to give money to states to offer drugs to poor seniors because they want a federal program for which they can claim credit.

``They have to stand for re-election in less than two years and they want

to have the credit for passing a prescription drug bill, more so than ... (sending) money to the states,'' he said.

-On a Medicaid loophole that has allowed the states to collect billions of extra dollars from Washington: He had to recuse himself from discussions because Wisconsin has an application pending to get in on the scheme that began when he was governor. ``Ask me about it in six months from now. I will tell you all you want to know about my transformation,'' he said.

-On the patients bill of rights: He's optimistic that a bill will pass Congress, saying the main sticking point now is not over the right to sue but over whether states can opt out of providing the protections.

-On Medicare contractors: He said Congress should change Medicare law to allow for more competition in choosing insurance companies to process claims and to allow for competitive pricing. ``That's going to be controversial as all get out,'' he said, ``but if you want us to do the job, give me the flexibility for contracting out for the best service possible.''

********* Health - Reuters - updated 10:29 AM ET Mar 28

Tuesday March 27 5:40 PM ET
HHS Secretary Likely to Change Privacy Rules

WASHINGTON (Reuters Health) - Health and Human Services (news - web sites) Secretary Tommy Thompson said Tuesday that changes to the Clinton administration regulations on the confidentiality of medical records are likely. Thompson did caution, however, that comments on the controversial rules are still coming in.

``I am fairly certain, without saying for sure, there will be some modifications to simplify and to lessen the financial burden,'' Thompson told health reporters at a breakfast meeting.

Thompson said he was moved to reopen the supposedly ``final'' rules after hearing from ``health entities across America about the tremendous burden of the privacy rules and regulations and the tremendous cost that is going to be foisted upon them.'' The rules had to be delayed for 60 days--until April 14--because of an error the Clinton administration made in transmitting them to Congress.

But Thompson assured reporters that there will be privacy regulations issued. ``There will be lots of
security placed in there so patients' rights and records will be protected,'' he said. And he even raised the
possibility that changes might not force a delay further than April 14--that the administration could publish
a ``final rule with amendments.''

The Clinton administration originally issued sweeping regulations to protect patient confidentiality in
December of 2000. They were the first ever to establish national standards for how personal health
information is used and distributed, and to set criminal and civil penalties for breaching patient privacy.

Consumer advocates hailed the privacy regulations for giving people unprecedented access to and control
over their personal medical information. HMOs, however, expressed concern that the regulations would
be too costly and complicated to implement effectively. Health plans also argued that health care costs
would rise drastically if they were forced to spend large sums of money to comply with the regulations.

********** [hipaalive] RE: SECURITY: OPERATIONAL AUDITS **********
>>> bsweeney@brishosp.chime.org 03/28/01 08:27AM >>>
*** This is HIPAAlive! From Phoenix Health Systems ***

We are going to perform similar "audits" in our hospital. The way we will handle it is to perform "rounds" similar to what we do now for safety. Every area will be put on a schedule and a small group of Information Security Council members will tour the area. These inspections will be unannounced to the area where they are taking place, and will be graded as compliant or non-compliant. Since there will be more than one person involved in doing the actual inspecting, there will need to be a consensus on how each item is graded. The department will be given a report card of sorts and have a specific amount of time to correct any non-compliant grades. Also included will be any recommendations the group feels are necessary. The Department Head is ultimately responsible, but if particular employees are noted as having problems following the rules, they will need to repeat information security & privacy training.
Betsy Sweeney
Project Administrator
Bristol Hospital and Health Care Group

bsweeney@brishosp.chime.org

-----Original Message-----
From: Odom, Melanie [``Thamailto:MSOdom@forrestgeneral.com]
Sent: Tuesday, March 27, 2001 4:55 PM
To: HIPAAlive Discussion List
Subject: [hipaalive] SECURITY: OPERATIONAL AUDITS

Would like some feedback regarding operational (Procedural) audits done in hospital facilities on privacy.
I am in a large hospital facility. Indicators that I am evaluating include:

1. Are employees signing on/off computers correctly?
2. Are privacy screens being utilized in workstations so that the general public cannot view?
3. Are paper records left open, displayed or accessible to unauthorized personnel?
4. Are employees noted sharing passwords?
5. Are employees noted failing to sign off upon completion of work?
6. Are screen savers being utilized?
7. Are monitors positioned in the workstations where unauthorized users cannot view?
8. Are monitors positioned in the patient rooms and other areas where unauthorized users cannot view?
9. Is staff using correct destruction process for patient information?
10. Are there bulletin boards or white boards with patients names where unauthorized personnel can view?
11. Does the unit/dept. demonstrate sound privacy practices overall?
12. When you receive a request for a fax, are you given and appropriate reason for a fax? Do you verify the information before it is sent?
Do you send only what is necessary to fulfill the need for information?

Please give me some feedback on ways that you might be doing this in your institution. What other indicators should be looked
for? The way we are evaluating these indicators is low compliance, compliant, and high compliance. The problem is, I may feel a unit is low compliant in one area but someone else may walk in the same unit and say they are compliant.

The way I look at it, you are either compliant or you're not . Right?!! But how can you put this on a scale. Can someone
help, or give me some ideas..

>>> mary.cooley@rsacompanies.com 03/28/01 09:56AM >>>
*** This is HIPAAlive! From Phoenix Health Systems ***

Melanie -

Unless your goal is to be able to determine the risk of any one item in a department from only the rating (i.e. low, compliant, high), I would suggest that you:
- Determine what the organization considers "compliant" and document it as a baseline in
  a database or spreadsheet for each question you list. This is your thought that it is
  either "compliant" or "not compliant"
- Determine whether ANY difference "is acceptable" or "not acceptable" to the
  organization
- During your assessment, make notes if a department does something similar, but
  different from the organization's definition of compliant. Also note the reasons why
  they do it differently
- Evaluate whether the alternate process meets the compliance definition
- Evaluate the risk to the organization of having more than one process/procedure for
  the same activity versus the estimated cost (time and complexity) to repair/change the
  process
- Rank that item with all of the others you determine are risks from your assessment

The risk of having more than one "acceptable" process for instance might be:
 - you would have to maintain/update two procedures in case of a mandated policy change
 - might cause operational confusion for transferred or loaned employees between
   departments and increase risk of critical errors
 - one or the other process might not be deemed acceptable to a major business associate
   or government entity
 - support functions (i.e. on-line support and computer services) would need to be aware
   and be able to handle the differences between the two processes
 - awareness training would need to be developed to identify the differences for ALL
   employees etc.

Once you have gone through this exercise, you will have a good idea at whether you need to change the process/system to conform and how urgent the

change is relative to other changes identified. If you decide on conformance, then it goes in to the estimation pot so that you can determine the method of change and the cost and develop a plan/schedule to remediate it.

A good example might be the use of password protected screen savers. If the organization considers compliance to be a mandatory screen saver with reversion to the screen saver at 30 seconds of non-use and one department has a computer in a locked office (say a pharmacy dispensing room) with the screen saver password, active and set at 10 minutes of non-use. Only two people have access to the room via keycard and a strict policy on never loaning out the keycard, is that a big risk? To the network, low risk, to the procedure for dispensing drugs, low risk, to the organization as a whole because of maintaining knowledge of policy in all affected departments and random enforcement action, moderate-high risk, to the IT security people responsible for managing the security procedures for computer resources, moderate-high risk. If you lay all of the tasks/functions out on a database or spreadsheet and evaluate each one for risk/impact, you will be able to see what the first, middle and last remediation tasks are and you will have initial audit documentation for comparison at a later date. You will also have a picture of where your control points are for the various processes.

In many of the organizations I work with, adherence to the policy is considered the minimum compliance and this difference would be eliminated to simplify the tracking and audit function, but in some organizations, mitigating factors are considered and differences are allowed primarily when the reason is faster response to patient care emergencies. It depends on your appetite for tracking and documenting the different processes and the reasons for them. In the HIPAA Privacy regulation world, you will have to know what you do and why and be able to explain why you consider the process compliant.

MC
Mary Cooley
Manager
Strategic Solutions
RSA Companies

==========